

Randomness, pseudorandomness and models of arithmetic

dedicated to Alan Woods

Pavel Pudlák*

October 18, 2012

Abstract

Pseudorandomness plays an important role in number theory, complexity theory and cryptography. Our aim is to use models of arithmetic to explain pseudorandomness by randomness. To this end we construct a set of models \mathcal{M} , a common element ι of these models and a probability distribution on \mathcal{M} , such that for every pseudorandom sequence s , the probability that $s(\iota) = 1$ holds true in a random model from \mathcal{M} is equal to $1/2$.

1 Introduction

A pseudorandom sequence is an infinite sequence of -1 s and 1 s computable in nondeterministic polynomial time that is not correlated with any polynomial time computable function. Such sequences can also be viewed as sets in $\mathbf{NP} \cap \mathbf{coNP}$; thus we can also talk about pseudorandom sets. Intuitively, a pseudorandom set splits every set in \mathbf{P} into two sets of equal density. There are some natural and important candidates for pseudorandom sequences in

*Partially supported by grants IAA100190902 of GA AV ČR and GAP202/12/G061 of GA ČR.

number theory such as the Liouville function (closely related to the Möbius function).

Our main result is a construction of a set of models \mathcal{M} , a common element ι of these models and a probability distribution on \mathcal{M} , such that for every pseudorandom sequence s , the probability that $s(\iota) = 1$ holds true in a random model from \mathcal{M} is equal to $1/2$. Thus pseudorandomness of sequences manifests itself in \mathcal{M} as genuine randomness. Admittedly, this result is weak, because it concerns only one common element of the models. We present it as a proof of the concept that results of this kind are possible. We suggest some ways of extending this result in Section 4.

We prove our result by using restricted ultrapowers, which are ultrapowers in which the sets of the ultrafilter and the functions are elements suitable classes. The history of restricted ultrapowers goes back to Skolem (see [5]). We will start with a model M_0 , a core of our construction, constructed from the set of all polynomial time computable functions reduced by a suitable ultrafilter on the complexity class \mathbf{P} . By extending the class of functions and the ultrafilter in various ways, we obtain a set of models \mathcal{M} extending the core model. Remarkably, there is a natural way of defining a probability measure on \mathcal{M} .

In the last section we present some philosophical speculations about the nature of pseudorandomness.

2 Preliminaries

2.1 Random sequences

We will study sequences $s : \mathbb{N} \rightarrow \{\pm 1\}$. Let \mathcal{S} denote the set of all such sequences with the uniform distribution. Intuitively, $Pr[s(n) = 1] = Pr[s(n) = -1] = \frac{1}{2}$ and these events are independent for different numbers. Formally, there is a Lebesgue measure m on \mathcal{S} that is uniquely determined by

$$m(\{s \in \mathcal{S}; s(1) = a_1 \wedge \dots \wedge s(n) = a_n\}) = 2^{-n}$$

for all n and all strings a of ± 1 s. We say that a “random sequence satisfies P ,” if the probability that a random sequence satisfies P is 1. If a random sequence satisfies P_1, P_2, \dots , then it also satisfies $\bigwedge_i P_i$.

The basic fact about random sequences is the Law of Large Numbers

$$Pr \left[\lim_{n \rightarrow \infty} \sum_{i=0}^{n-1} s(i)/n = 0 \right] = 1.$$

This theorem, however, does not provide information about the rate of convergence. Much more precise theorems have been proven, in particular Khinchin's Law of Iterated Logarithm

$$Pr \left[\limsup_{n \rightarrow \infty} \sum_{i=0}^{n-1} s(i)/\sqrt{2n \ln \ln n} = 1 \right] = 1,$$

which, in particular, implies that for every $\epsilon > 0$,

$$Pr \left[\lim_{n \rightarrow \infty} \sum_{i=0}^{n-1} s(i)/n^{\frac{1}{2}+\epsilon} = 0 \right] = 1. \quad (1)$$

2.2 Algorithmic randomness

We want to formalize the concept that a sequence s “looks like a random sequence”. Here the sequence s is fixed, so we cannot use probability theory. The basic idea is that s must satisfy many properties that random sequences satisfy with probability 1. E.g., we certainly want the property used in the Law of Large Numbers. Further, we want to consider properties that can be algorithmically decided. Therefore it is more natural to talk about satisfying *tests* instead of properties.

The study of such concepts has long history and many researchers contributed to it, including Kolmogorov, Chaitin, Levin, Schnorr and Martin-Löf. This research area is called *algorithmic randomness*. We mention one of the concepts that is studied there, so that we can compare it with the concept that we will introduce.

A *martingale* is a function $F : \{\pm 1\}^* \rightarrow \mathbb{R}^+$ such that

$$F(a_1, \dots, a_n) = \frac{1}{2}(F(a_1, \dots, a_n, -1) + F(a_1, \dots, a_n, +1))$$

Definition 1 (Schnorr [8]) A sequence $s : \mathbb{N} \rightarrow \{\pm 1\}$ is **P**-random, if for every polynomial time computable martingale

$$\limsup_{n \rightarrow \infty} F(s(0), s(1), \dots, s(n-1)) < \infty.$$

Another concept relevant to this paper is the concept of *pseudorandom number generator*, which will be abbreviated by PRG. A PRG is an algorithm to produce a long string of numbers, usually just 0s and 1s, from a short random string, called the *seed*. So in this case we do not have only one infinite sequence, but a small set of finite strings with a probability distribution. This concept plays an important role in the theories that study computational complexity and cryptography.

There is one important difference in how the computational resources are bounded in the two mentioned approaches. When testing a sequence s for **P**-randomness, the testing algorithm receives the whole string $(s(0), s(1), \dots, s(n-1))$ as an input and can use time polynomial in n . In contrast, algorithms testing pseudorandomness get n represented in binary and can use time polynomial in the length of n , i.e., they run in time polynomial in $\log n$.

2.3 Pseudorandom sequences

Our concept is closer to the theory of pseudorandomness than to algorithmic randomness. That is why we use the word *pseudorandom*. The reader should, however, be cautioned that there are concepts with similar names that differ significantly from ours.

Definition 2 *A sequence $s : \mathbb{N} \rightarrow \{\pm 1\}$ will be called pseudorandom if*

1. *s is computable in nondeterministic polynomial time,*
2. *for every polynomial time computable function $f : \mathbb{N} \rightarrow \{\pm 1\}$,*

$$\lim_{n \rightarrow \infty} \sum_{i=0}^{n-1} f(i)s(i)/n = 0. \quad (2)$$

Condition 1. means that although we may be not able to compute the value $s(n)$ in polynomial time, if somebody gives us a “witness” we are able to check the correct value of $s(n)$ in polynomial time. (There should always be witnesses for either the value 1 or the value -1 , but never for both.) We can identify s with the set $\{n; s(n) = 1\} \in \mathbf{NP} \cap \mathbf{coNP}$, so we can also talk about *pseudorandom sets*.

Condition 2. means that s is little correlated with any sequence computable in polynomial time. One can consider various modifications of this

condition. For instance, one can allow stronger tests, say, functions computable in appropriately defined subexponential time. One can also impose stronger bounds on correlation. If, for example, we required that

$$\lim_{n \rightarrow \infty} \sum_{i=0}^{n-1} f(i)s(i)/n^\alpha = 0,$$

for some $1/2 < \alpha < 1$, then the correlation would be exponentially small (on finite initial segments; recall that the input size is $\log n$).

Another motivation for the definition above is the *Möbius Randomness Principle* proposed by Peter Sarnak (see [4]). According to this principle the Möbius function μ is not correlated to any “low-complexity” function $F : \mathbb{N} \rightarrow [-1, 1]$ in the sense that

$$\lim_{n \rightarrow \infty} \sum_{i=1}^n F(i)\mu(i)/n = 0.$$

This is like saying that μ is pseudorandom, except for a few minor differences. First, μ takes on not only the values ± 1 , but also 0. This does not seem very important for studying the concept of pseudorandomness (see Proposition 2.3 below). Second, it is not specified what “low complexity” means. This leaves open the possibility of studying various specific versions of the conjecture. Third, the tests are functions F whose range is in the whole interval $[-1, 1]$. We will show below that this is also an irrelevant difference.

Proposition 2.1 *Suppose that $s : \mathbb{N} \rightarrow \{\pm 1\}$ is pseudorandom. Let $F : \mathbb{N} \rightarrow [-1, 1]$ be a polynomial time computable function whose values are binary rationals. Then*

$$\lim_{n \rightarrow \infty} \sum_{i=1}^n F(i)s(i)/n = 0.$$

Proof. Let s and F be given. One can easily show that s is pseudorandom also with respect to polynomial time computable functions $f : \mathbb{N} \rightarrow \{-1, 0, 1\}$. (Hint: write $f = \frac{1}{2}f_+ + \frac{1}{2}f_-$, where $f_+(n) = 1$ if $f(n) = 1$, otherwise $f_+(n) = -1$, and $f_-(n) = -1$ if $f(n) = -1$, otherwise $f_-(n) = 1$.)

Represent F as a weighted sum of such functions, $F(n) = \sum_{j=0}^{\infty} 2^{-j} f_j(n)$. Then

$$\lim_{n \rightarrow \infty} \sum_{i=1}^n F(i)s(i)/n = \lim_{n \rightarrow \infty} \sum_{i=1}^n \sum_{j=0}^{\infty} 2^{-j} f_j(n)s(i)/n = \sum_{j=0}^{\infty} 2^{-j} \lim_{n \rightarrow \infty} \sum_{i=1}^n f_j(n)s(i)/n = 0$$

because the infinite sum converges absolutely. ■

Say that a set of numbers A has *positive density*, if $\liminf_{n \rightarrow \infty} |A \cap [0, n-1]|/n > 0$.

Corollary 2.2 *If X is a pseudorandom set, then neither X nor its complement contains a set $A \in \mathbf{P}$ of positive density.*

A possible way of stating the Möbius Randomness Principle is to say that μ is pseudorandom in the sense of our definition (extended to sequences of -1 , 0 and 1). A closely related function is the Liouville function λ . It is defined by $\lambda(n) = (-1)^k$, where k is the number of prime factors of n counted with their multiplicity.

Proposition 2.3 *μ is pseudorandom if and only if λ is.*

Proof. 1. Suppose μ is pseudorandom. Let a polynomial time computable function $f : \mathbb{N} \rightarrow \{\pm 1\}$ and $\epsilon > 0$ be given. Let n_0 be such that $\sum_{k > n_0} k^{-2} < \epsilon$. We have

$$\begin{aligned} & \left| \lim_{n \rightarrow \infty} \sum_{i=1}^n f(i)\lambda(i)/n \right| \leq \\ & \sum_{1 \leq k \leq n_0} \left| \lim_{n \rightarrow \infty} \sum_{\substack{1 \leq k^2 i \leq n, \\ i \text{ square free}}} f(k^2 i)\lambda(k^2 i)/n \right| + \sum_{k > n_0} \left| \lim_{n \rightarrow \infty} \sum_{\substack{1 \leq k^2 i \leq n, \\ i \text{ square free}}} f(k^2 i)\lambda(k^2 i)/n \right| < \\ & \sum_{1 \leq k \leq n_0} \left| \lim_{n \rightarrow \infty} \sum_{1 \leq k^2 i \leq n} f(k^2 i)\mu(i)/n \right| + \epsilon = \epsilon. \end{aligned}$$

2. Now suppose that μ is not pseudorandom. Let $f : \mathbb{N} \rightarrow \{\pm 1\}$ be a polynomial time computable function and $\epsilon > 0$ such that $\lim_{n \rightarrow \infty} \sum_{i=1}^n f(i)\mu(i)/n = \epsilon$. Let n_0 be as above. Furthermore, we can suppose that $\lim_{n \rightarrow \infty} \sum_{i=1}^n f(i)\lambda(i)/n = 0$, because otherwise we would be done. In a similar fashion as above, decompose the $\sum_{i=1}^n f(i)\lambda(i)/n$ into three terms

1. the sum over square free numbers i ,
2. the sum over numbers i divisible by k^2 for some $k \leq n_0$, and
3. the sum over the remaining numbers i .

By our assumptions, the limit of the first sum is ϵ , the sum of the limits of the sums 2. and 3. is $-\epsilon$, the sum 3. is $> -\epsilon$. Hence, if we define

$$g(n) = \begin{cases} -f(n) & \text{if } n \text{ is divisible by } k^2 \text{ for some } k \leq n_0, \\ f(n) & \text{otherwise,} \end{cases}$$

we obtain $\lim_{n \rightarrow \infty} \sum_{i=1}^n g(i)\lambda(i)/n > 0$. ■

Some special cases of the Möbius randomness principle have been proven. The first one was the Prime Number Theorem, which is the case of $f \equiv 1$. (The question whether the bound on correlation can be improved to the form (1) is the Riemann Hypothesis.) Recently B. Green proved the principle for AC^0 , [4]. Let us say that a sequence is AC^0 -pseudorandom if it satisfies Definition 2 with the condition 2. weakened to AC^0 -computable. Then one can state Green's result as follows.

Theorem 2.4 ([4]) *The Möbius function is AC^0 -pseudorandom.*

The Liouville function is also AC^0 -pseudorandom.

It will be very difficult to prove that some sequence is pseudorandom, because the existence of pseudorandom sequences implies $\mathbf{P} \neq \mathbf{NP}$. For specific functions, it may be even harder. If the Möbius function is pseudorandom, then integers cannot be factored in polynomial time.

In the opposite direction, we know that hardness of factoring implies the existence of pseudorandom sequences (we are not able to prove that it implies the pseudorandomness of the Möbius function, though). This is because

1. there are constructions of permutations that are *one-way functions* provided that factoring is hard,
2. there is a construction of a *hard-core predicate* from any one-way permutation, and
3. hard-core predicates are very closely related to pseudorandom sequences.

We will now explain this connection in more detail, but for the sake of brevity, we will skip the definition of a one-way function. Let $1 \leq k_1 < k_2 < \dots$ be a sequence of integers that grow at most polynomially, and let $F_j : \{0, 1\}^{k_j} \rightarrow \{0, 1\}^{k_j}$, $j = 1, 2, \dots$, be a sequence of permutations. Suppose that these numbers and functions are uniformly computable in polynomial

time. We say that functions $B_j : \{0, 1\}^{k_j} \rightarrow \{0, 1\}$, $j = 1, 2, \dots$, are hard-core predicates for the functions F_j , if B_j are uniformly computable in polynomial time, and for every function $g(x)$ computable by a randomized polynomial time algorithm

$$\Pr[g(F_j(x)) = B_j(x)] = \frac{1}{2} \pm \frac{1}{k_j^{\omega(1)}}, \quad (3)$$

where the probability is taken over uniformly distributed $x \in \{0, 1\}^{k_j}$ and random bits of the algorithm for g ; further, $\omega(1)$ is the standard notation for functions going to infinity. In plain words, this means that $B_j(x)$ can be predicted from $F_j(x)$ only with negligible probability (which, in particular, implies that it is difficult to invert F_j).

The concept that is closely related to pseudorandom sequences (as defined in this paper) is the sequence $B_j(F^{-1}(y))$, $j = 1, 2, \dots$. To get a pseudorandom sequence s , we only need to connect the bits $B_j(F^{-1}(y))$ into one infinite sequence:

$$s(n) = (-1)^{B_j(F^{-1}(n - \sum_{i < j} 2^{k_i}))},$$

where $\sum_{i < j} 2^{k_i} \leq n < \sum_{i \leq j} 2^{k_i}$ and where we are identifying $\{0, 1\}^{k_j}$ with $0, 1, \dots, 2^{k_j} - 1$.

In order to show that $s(n)$ is pseudorandom, we have to address only one small complication. While in (2) of the definition of pseudorandomness we consider all initial segments, in (3) of the definition of the hard-core predicate we only consider correlation over the entire interval $[0, 2^{k_j} - 1]$ (but we have better convergence). We need to show that the correlation of $B_j(F^{-1}(y))$ with polynomial time functions is also low on an initial segments $[0, a]$ of $[0, 2^{k_j} - 1]$.

Suppose g has positive correlation with $B_j(F^{-1}(y))$ on $[0, a]$. If we knew a , we could define g' that has positive correlation with $B_j(F^{-1}(y))$ on the entire interval by putting $g'(x) = g(x)$ on $[0, a]$ and $g'(x) = 1 - g(x)$ on the rest. Since we cannot assume that we know a , we have to do something slightly more complicated. Note that we are actually assuming that there are infinitely many indices j for which g has positive correlation with $B_j(F^{-1}(y))$ on some interval $[0, a_j]$. The ratios $a_j/2^{k_j}$ have some limit point α , $0 < \alpha < 1$. Take a rational number β close to α (or α itself if it is rational). Then use $\lceil \beta 2^{k_j} \rceil$ as switching points.

This finishes a sketch of the proof of the following proposition.

Proposition 2.5 *If there exists no probabilistic polynomial time algorithm*

for factoring integers, then there exists a pseudorandom sequence.

Remarks. 1. The construction actually gives a concrete sequence, but since its definition is rather complicated, we do not present it here.

2. We have not fully used the assumption about factoring; one can show pseudorandomness of the constructed sequence in a little stronger sense.

3. For the concepts and results used above, see [3].

2.4 Theories

We need a theory in which it is possible to formalize polynomial time computations. A natural theory in which this is possible is Cook's PV , [1, 6]. This theory has function symbols for all polynomial time computable function. The function symbols correspond to algorithms based on recursion on notation. Our result is quite general and, as such, holds for the stronger theory $PV^{\mathbb{N}}$ defined below.

Definition 3

1. $PV^{\mathbb{N}}$ is the theory axiomatized by all true universal sentences in the language of PV .
2. $AR^{\mathbb{N}}$ is the theory consisting of all true sentences in the language of PV .

The theory $PV^{\mathbb{N}}$ is a conservative extension of the theory of all true Π_1^0 arithmetical sentences plus the axiom $\forall x \exists y \ y = x^{\lceil \log(x+1) \rceil}$ (this axiom guarantees that the provably total functions grow sufficiently fast and thus enable us to define polynomial time computations). The theory $AR^{\mathbb{N}}$ is essentially *True Arithmetic*, except that we use the richer language of PV .

We focus on the complexity class \mathbf{P} , as this is the most interesting case, but in fact the same result can be proven for concepts based on other classes. An interesting case is the class \mathbf{AC}^0 because of the result of Green mentioned above. The theory corresponding to this class is V^0 , see [2].

2.5 Random models

Our aim is to represent pseudorandomness in a different way. The basic idea is to study this concept using a set of nonstandard models equipped with a

probability distribution. Let σ be a first order formula in the language of PV defining a sequence $s \in \mathcal{S}$, and suppose that we have a set of models \mathcal{M} with a probability distribution ν . Let ϕ be a first order formula. Then we can say ‘ s satisfies the property ϕ with probability p ’ if the probability that in a random model from \mathcal{M} the sequence defined by σ satisfies ϕ is p .

If we want to use formulas ϕ with parameters, i.e., free variables for elements of models, we need to impose some structure on \mathcal{M} . In this paper we will only consider the following structure. There is one distinguished model M_0 such all other models are its extensions. This enables us to speak about properties parameterized by elements of M_0 .

In this paper we say that a model N is an *extension* of a model M , if M is a substructure of N .

In general the structure defined on \mathcal{M} can be more complicated. We can use various frames, like in the Kripke semantics. If N is one of the “alternative worlds” of M , then N should be an extension of M (not necessarily proper).

An alternative approach is to use a Boolean valued model M with a boolean algebra \mathcal{B} equipped with a probability measure, an approach studied in [7]. This is, however, not fundamentally different from the approach sketched above. Having such a model, we can construct a set of models by taking all ultrafilters on \mathcal{B} . Vice versa, having \mathcal{M} and ν as above, we can take the Boolean algebra of measurable subsets of \mathcal{M} and define a measure on this algebra in a natural way.

3 The result

Theorem 3.1 *There exists a model M_0 of $PV^{\mathbb{N}}$, an element $\iota \in M_0$, a set \mathcal{M} of models of $AR^{\mathbb{N}}$ and a probability measure ν on a sigma algebra \mathcal{B} of subsets of \mathcal{M} such that*

1. *models of \mathcal{M} are extensions of M_0 ,*
2. *for every PV formula $\phi(x_1, \dots, x_k)$ and every string of elements $a_1, \dots, a_k \in M_0$, the set $\{M \in \mathcal{M}; M \models \phi(a_1, \dots, a_k)\}$ is in \mathcal{B} ,*
3. *for every (definition of a) pseudorandom sequence s ,*

$$Pr_{\nu}[M \models s(\iota) = 1] = \frac{1}{2}.$$

Proof. Let $K \subseteq \mathbb{N}$ be an infinite set. We define *density of sets of numbers with respect to K* , or *K -density*, to be the partial function defined by

$$\text{dens}_K X = \lim_{k \in K, k \rightarrow \infty} \frac{|X \cap [0, k-1]|}{k}. \quad (4)$$

($\text{dens}_K X$ is undefined when the limit does not exist.)

The proofs of the following easy facts are left to the reader.

1. dens_K is finitely additive.
2. If $\text{dens}_K X = \text{dens}_K Y = 1$, then $\text{dens}_K X \cap Y = 1$.
3. If C is a countable set of sets of numbers, then there exists an infinite K such that $\text{dens}_K X$ is defined (i.e., the limit (4) exists) for every $X \in C$.

Let \mathbf{AR} denote arithmetically definable sets of natural numbers (which is the same as sets first-order definable in the language of PV). Let K be an infinite set of numbers such that $\text{dens}_K X$ is defined for every $X \in \mathbf{AR}$.

The following fact is also easy.

4. Let $X \in \mathbf{P}$ and Z be a pseudorandom set. Then $\text{dens}_K X \cap Z = \frac{1}{2} \text{dens}_K X$.

Let \mathcal{F}_0 be the filter in \mathbf{P} consisting of all sets of K -density 1. Let \mathcal{U}_0 be an ultrafilter extending \mathcal{F}_0 . Hence all sets in \mathcal{U}_0 have positive density. Let \mathbf{FP} denote the set of functions computable in polynomial time. We define M_0 to be the ultrapower constructed by taking \mathbf{FP} modulo \mathcal{U}_0 ,

$$M_0 = \mathbf{FP}/\mathcal{U}_0,$$

with the PV function symbols interpreted in the natural way. The fact in M_0 all true universal PV sentences are satisfied is an immediate consequence of Łoś's theorem. The distinguished element $\iota \in M_0$ is defined to be the element of $\mathbf{FP}/\mathcal{U}_0$ represented by the identity function id on \mathbb{N} , in symbols $\iota = [id]_{\mathcal{U}_0}$.

Let $u_0 = \{U_1 \supset U_2 \supset \dots\}$ be a cofinal chain in \mathcal{U}_0 . We define the *density of a set with respect to u_0* , or *u_0 -density*, to be the partial function defined by¹

$$\text{dens}_{u_0} X = \lim_{n \rightarrow \infty} \frac{\text{dens}_K X \cap U_n}{\text{dens}_K U_n}. \quad (5)$$

¹More precisely, we should also use the index K , but there is no danger of confusion, since K is fixed for the rest of the proof.

Again, one can easily prove that we can pick u_0 so that u_0 -density is defined for every $X \in \mathbf{AR}$. The following facts are immediate corollaries of 1. and 4.:

- 5. dens_{u_0} is finitely additive.
- 6. $\text{dens}_{u_0} Z = \frac{1}{2}$ for every pseudorandom set Z .

The set of models that extend M_0 will be defined using the following set of ultrafilters on the boolean algebra \mathbf{AR} .

$$\Omega = \{\mathcal{U}; \mathcal{U} \text{ ultrafilter on } \mathbf{AR}, \mathcal{U}_0 \subseteq \mathcal{U} \text{ and } \forall V \in \mathcal{U} \text{ dens}_{u_0} V > 0\}.$$

- 7. If $\mathcal{F} \subseteq \mathbf{AR}$ is a filter such that $\text{dens}_{u_0} U > 0$ for all $U \in \mathcal{F}$, then \mathcal{F} can be extended to an ultrafilter belonging to Ω .

Let \mathbf{FAR} denote arithmetically definable functions. Define

$$\mathcal{M} = \{M; M = \mathbf{FAR}/\mathcal{U}, \mathcal{U} \in \Omega\}.$$

Note that for $\mathcal{U}_1 \neq \mathcal{U}_2$, the ultrapower models are different (they may be isomorphic, though). Since $\mathbf{FP} \subseteq \mathbf{FAR}$ and $\mathcal{U}_0 \subseteq \mathcal{U}$, for every $\mathcal{U} \in \Omega$, we have:

- 8. Every $M \in \mathcal{M}$ is an extension of M_0 .

The fact that these models are models of True Arithmetic, is a well-known consequence of Łoś's theorem.

For $X \in \mathbf{AR}$, let

$$\Omega[X] = \{\mathcal{U}; X \in \mathcal{U}\},$$

and put

$$\mathcal{A}_0 = \{\Omega[X]; X \in \mathbf{AR}\}$$

- 9. \mathcal{A}_0 is a Boolean algebra.

Lemma 3.2 $\Omega[X] = \Omega[Y]$ if and only if $\text{dens}_{u_0} X \triangle Y = 0$ (where \triangle denotes the symmetric difference).

Proof. $\text{dens}_{u_0} X \setminus Y > 0$. Let \mathcal{F} be the filter in \mathbf{AR} generated by $X \setminus Y > 0$. By 7., \mathcal{F} has an extension to $\mathcal{U} \in \Omega$. Hence $\mathcal{U} \in \Omega[X] \setminus \Omega[Y]$. This gives us the forward implication.

Now suppose $\mathcal{U} \in \Omega[X] \setminus \Omega[Y]$, for some \mathcal{U} . Then $X \setminus Y \in \mathcal{U}$. Since ultrafilters in Ω do not contain sets of u_0 -density 0, we have $\text{dens}_{u_0} X \setminus Y > 0$.

■

This lemma enables us to define an additive measure ν_0 on \mathcal{A}_0 by putting

$$\nu_0(\Omega[X]) = \text{dens}_{u_0} X.$$

In particular, $\nu_0(\Omega) = 1$.

Lemma 3.3 *If $A_1, A_2, \dots \in \mathcal{A}_0$ are pairwise disjoint and $\bigcup_n A_n \in \mathcal{A}_0$, then $\nu_0(A_n) = 0$ for all n except for a finite number of them.*

Proof. To prove the claim, suppose the contrary. Let $X, X_1, X_2, \dots \in \mathbf{AR}$ be such that $A_n = \Omega[X_n]$, for $n = 1, 2, \dots$, and $\bigcup_n A_n \in \mathcal{A}_0$. We observe that $\text{dens}_{u_0} X_i \cap X_j = 0$ for $i \neq j$, because $A_i \cap A_j = \emptyset$.

Let $Y_n = X \setminus \bigcup_{i=1}^{n-1} X_i$. We will show that $\text{dense}_{u_0} Y_n > 0$ for all n . Suppose that for some n , $\text{dense}_{u_0} Y_n = 0$. Let $m \geq n$ such that $\text{dens}_{u_0} X_m > 0$. Since $\text{dens}_{u_0} X_m \cap \bigcup_{i=1}^{n-1} X_i = 0$, we have $\text{dens}_{u_0} X_m \cap X = 0$. This implies that $\Omega[X_m] \cap \Omega[X] = \emptyset$. But this is impossible, because $\Omega[X_m] \neq \emptyset$. Thus $\text{dense}_{u_0} Y_n > 0$ for all n .

Extend the filter $\{Y_n; n = 1, 2, \dots\}$ to an ultrafilter $\mathcal{U} \in \Omega$. Clearly $\mathcal{U} \in \Omega[X]$, but for no n , $\mathcal{U} \in \Omega[X_n]$. ■

An immediate corollary is:

10. ν_0 is σ -additive.

According to a basic theorem about extensions of measures, we can extend the σ -additive probability measure ν_0 defined on the Boolean algebra \mathcal{A}_0 to a σ -additive probability measure ν_1 defined on a σ -algebra \mathcal{A}_1 . Using the bijection $\mathcal{U} \mapsto \mathbf{FAR}/\mathcal{U}$ we translate the measure ν_1 defined on a σ -algebra \mathcal{A}_1 to a measure ν defined on a σ -algebra \mathcal{B} of subsets of \mathcal{M} .

We will now prove the second condition of the theorem. Let $\phi(x_1, \dots, x_k)$ be a PV formula, $a_1, \dots, a_k \in M_0$, let $\mathcal{U} \in \Omega$ and let $M = \mathbf{FAR}/\mathcal{U}$. Further, let $f_1, \dots, f_k \in \mathbf{FAR}$ be the functions representing a_1, \dots, a_k (in symbols, $a_i = [f_i]_{\mathcal{U}_0}$).

According to Łoś's theorem, $M \models \phi(a_1, \dots, a_k)$ if and only if

$$\{n; \mathbb{N} \models \phi(f_1(n), \dots, f_k(n))\} \in \mathcal{U}.$$

Hence the set of ultrafilters for which the models satisfy $\phi(a_1, \dots, a_k)$ has the form $\Omega[X]$, for $X \in \mathbf{AR}$. Therefore

$$\{M; M \models \phi(a_1, \dots, a_k)\} \in \mathcal{B}.$$

It remains to prove the third condition of the theorem. Let s be a pseudorandom sequence and let $\psi(x)$ be a formula defining $s(x) = 1$. By Łoś's theorem, the set of models satisfying $\psi(\iota)$ corresponds to the set of ultrafilters such that $\{n; \mathbb{N} \models \psi(n)\} \in \mathcal{U}$ (recall that $\iota = [id]_{\mathcal{U}_0}$). Thus we have

$$\begin{aligned} \nu(\{M; M \models \psi(\iota)\}) &= \nu_1(\{\mathcal{U}; \{n; \mathbb{N} \models \psi(n)\} \in \mathcal{U}\}) \\ &= \text{dens}_{u_0}\{n; \mathbb{N} \models \psi(n)\} \\ &= \frac{1}{2}, \end{aligned}$$

by 6. Thus the theorem is proved. ■

4 Remarks

1. We will generalize the concept of pseudorandom sequences and sets to cover sequences in which 1 occurs with frequency $p \neq \frac{1}{2}$.

Definition 4 *Let p be a real number, $0 < p < 1$. We will say that a sequence $s : \mathbb{N} \rightarrow \{\pm 1\}$ is p -biased pseudorandom, if s is computable in nondeterministic polynomial time and*

$$\lim_{n \rightarrow \infty} \sum_{i=0}^{n-1} f(i)((s(i) - 1)/2 + p) = 0,$$

for every polynomial time computable function $f : \mathbb{N} \rightarrow \{\pm 1\}$.

A set $X \subseteq \mathbb{N}$ will be called p -biased pseudorandom, if it is the set of arguments for which a p -biased pseudorandom sequence is 1.

Several propositions proved above generalize to p -biased pseudorandom sequences and sets. In particular, we would like to draw reader's attention to Corollary 2.2 and Theorem 3.1. The condition 3. of Theorem 3.1 holds true for all real numbers p , $0 < p < 1$ and all p -biased pseudorandom sequences simultaneously.

2. The main weakness of Theorem 3.1 is that condition 3. is stated only for one element, only for ι . One can show that in the constructed system \mathcal{M} , condition 3. holds for several other elements of M_0 ; in particular, it is true for all elements of the form $a\iota + b$ for $a \in \mathbb{N}$ and $b \in \mathbb{Z}$. This can easily be proved using the following lemma.

Lemma 4.1 *Let s be a pseudorandom sequence. Let $g \in \mathbf{FP}$ be increasing and invertible in polynomial time on an infinite interval $[n_0, \infty)$. Furthermore, suppose that $\text{Rng}(g)$, the range of g , has positive density. Then the sequence s' defined by $s'(x) = s(g(x))$ is also pseudorandom.*

Proof. Let s and g be given and suppose s' is not pseudorandom. Let f be a function that witnesses that s' is not pseudorandom. We define a function that witnesses that s is not pseudorandom.

$$f'(n) = \begin{cases} f(g^{-1}(n)) & \text{if } n \geq n_0 \text{ and } n \in \text{Rng}(g), \\ 0 & \text{otherwise.} \end{cases}$$

■

We certainly cannot expect condition 3. to hold for all numbers of M_0 . For small numbers n , $s(n)$ is defined in M_0 , because s is computable in exponential time. If $\alpha \in M_0$ is larger than all numbers $c\iota$, for $c \in \mathbb{N}$, then $\alpha = [g]\iota_0$ for some g that grows more than linearly. The range of such a g has density 0, hence we cannot deduce anything about it. For example, $\lambda(n^2) = 1$ for all n , whence $M_0 \models \lambda(\iota^2) = 1$.

3. We also cannot expect stronger properties of random sequences to hold in the system of models of Theorem 3.1 unless we assume more about the sequences. For example, $s(\iota)$ and $s(\iota + 1)$ do not have to be independent in \mathcal{M} , because we do not assume any kind of independence for pairs $s(n)$ and $s(n + 1)$, $n \in \mathbb{N}$. A more specific example (assuming that λ is pseudorandom) is the fact that $\lambda(2n) = -\lambda(n)$.

5 Philosophical speculations

Some cosmologists believe that when the universe emerged from a singularity some physical properties of it were decided randomly. Others even believe that there is a *multiverse* consisting of many different universes, one of which is our universe. In contrast to this, philosophers have never doubted that the basic mathematical structures, namely the natural and real numbers, are unique. These structures are unique in the sense that they must be same in all conceivable physical worlds.

There are good reasons to believe that the natural numbers are absolute in the sense that there are no possible alternatives to them. The only

structures that satisfy the basic arithmetical laws and are different from the natural numbers are nonstandard models. Though it has been proposed that the actual natural numbers have the structure of a nonstandard model, e.g., in [9], most philosophers do not accept such a possibility. The problem is that a nonstandard model contains the standard model as an initial part, and so we should identify the natural numbers with this initial part. Thus viable alternatives should use the same numbers with different arithmetical operations. Since we can prove that the operations of addition and multiplication are uniquely determined by the basic axioms (the axioms of Robinson Arithmetic), it is inconsistent to assume that on the set of standard numbers different kinds of addition and multiplication are possible.

However, what is inconsistent in our world may be consistent in a different one, and vice versa. Consider a pair of (necessarily nonstandard) models of Peano Arithmetic M and N that have the same elements, the same addition, but different multiplication. (Such pairs can be easily constructed using recursively saturated models.) In a world in which M is the standard natural numbers, it is inconsistent to assume that anything like N exists. Yet, it does.

We may secretly ponder over such scenarios, but there is a strong reason not to talk about the possibility of different arithmetics openly. If a concept is inconsistent, we cannot talk about it and there cannot be any theory around it. Therefore, any conjecture of this kind would be neither provable nor disprovable and, as such, should be discarded as meaningless.

However, some phenomena can be studied even if they are not directly observable—because they have side effects. The presence of these effects is a proof of the phenomenon. A side effect of the origin of our integers in a random process could be the randomness present in the structure of integers. It is not genuine randomness, because the integers are a single structure. What we rather observe are some properties that are satisfied by truly random objects. Therefore we call it *pseudorandomness*. Number theorists are familiar with this; they use assumptions about random behavior in heuristic arguments when they are not able to prove theorems rigorously and some conjectures are also justified in this way (including the Riemann Hypothesis).

Acknowledgment

We would like to thank Emil Jeřábek and Jan Krajíček for their useful comments and suggestions.

References

- [1] S.A. Cook: Feasibly constructive proofs and the propositional calculus. In: Proc. seventh annual ACM symposium on Theory of computing, ACM New York, 83–97, (1975)
- [2] S.A. Cook, P. Nguyen: Logical Foundations of Proof Complexity. ASL series Perspectives in Logic, Cambridge Univ. Press, (2010)
- [3] O. Goldreich: Foundation of Cryptography: Basic Tools. Cambridge Univ. Press, (2001)
- [4] B. Green: On (not) computing the Möbius functions using bounded depth circuits. Combinatorics, Probability and Computing, to appear
- [5] S. Kochen, S. Kripke: Non-standard models of Peano arithmetic. In: Logic and arithmetic, int. Symp., Zrich 1980. Enseign. Math., II. Sér. 28, 211–231, (1982)
- [6] J. Krajíček: Bounded arithmetic, propositional logic, and complexity theory. Encyclopedia of Mathematics and Its Applications, Vol.60, Cambridge University Press, Cambridge - New York - Melbourne, (1995)
- [7] J. Krajíček: Forcing with random variables and proof complexity. London Mathematical Society Lecture Note Series, No.382, Cambridge University Press, (2011)
- [8] C.P. Schnorr: A unified approach to the definition of a random sequence. Mathematical Systems Theory 5(3), 246–258, (1971)
- [9] P. Vopěnka: Mathematics in the Alternative Set Theory. Teubner, Leipzig (1979)